Prepared testimony of
Paul B. Kurtz
Executive Director
The Cyber Security Industry Alliance

Before the Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity
of the
House Committee on Homeland Security

"The Future of Cyber and Telecommunications Security
at the Department of Homeland Security"

2212 Rayburn House Office Building
Wednesday, Sept. 13, 2006

Introduction

Chairman Lungren, Ranking Member Sanchez and members of the Subcommittee, thank you for the opportunity to testify today before the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. My name is Paul Kurtz and I am Executive Director of the Cyber Security Industry Alliance (CSIA).

CSIA is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. It is our belief that a comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security and economic stability.

Before joining CSIA, I served at the White House on the National Security Council and Homeland Security Council. On the NSC, I served as Director of Counterterrorism and Senior Director of the Office of Cyberspace Security. On the HSC, I was Special Assistant to the President and Senior Director for Critical Infrastructure Protection.

My testimony will address four themes for consideration by Congress on refining the role of the Department of Homeland Security as it relates to national cyber security:

- Inadequate attention
- Lack of leadership
- No plan to prevent or minimize a major cyber disaster
- No plan for working with the private sector to recover from a cyber disaster

Cyber Security is Receiving Inadequate Attention from DHS

Last week in his updated national strategy for counterterrorism, President George W. Bush declared that "America is safer but we are not yet safe." The reality of physical terror occurring in the United States of America has riveted our attention since the attacks on September 11, 2001. Prevention of any physical incident of horror has since been priority one.

The President's reminder for vigilance clearly applies to threats against our physical well-being, but his admonition must also apply to the threats against cyber security. To some the idea of terrorists or hackers breaking into computers may sound like an abstract threat, especially when compared to the shock of a suicide bomber killing innocent people and destroying property. However, a successful massive cyber attack could trigger grave harm for many Americans if it knocked out communications and information systems for emergency response, energy, transportation, and other critical resources that depend on IT. The nation experienced such vivid fallout from a regionalized natural disaster last year in the aftermath of Hurricane Katrina – imagine this disaster on a national scale.

Since 9/11, responsibility for coordinating federal efforts on national safety shifted to the Department of Homeland Security. DHS has predictably reacted to a myriad of security challenges by focusing first on immediate physical threats. This focus is understandable, but it

has also impeded progress toward stronger national cyber security. As a result, the United States remains unprepared to defend itself against a massive cyber attack or to systematically recover and reconstitute information systems after a successful attack.

My testimony will describe what DHS is and is not doing with respect to national cyber security, plus the need for DHS to specify how it and the private sector would coordinate actions if a massive cyber attack were to occur. By realistically refining the Department's role in national cyber security, DHS can escalate cyber security efforts in concert with efforts to prevent physical terror in America.

There is no leadership at DHS for national cyber security

Despite publication of more than 750 pages of strategies, directives and response plans, leadership in the U.S. government on cyber security is clearly absent. The practical significance of lack of leadership means the nation is not ready for a major disruption to our information infrastructure.

National coordination of cyber security is the purview of the Department of Homeland Security, and its related leadership position is Assistant Secretary for Cyber Security and Telecommunications. This new position was established in July 2005 by Secretary Chertoff specifically to elevate the importance of cyber security in relation to DHS's main focus on physical security. Unfortunately, fourteen months later, the Assistant Secretary position is unfilled, which reflects the low priority DHS still has toward cyber security. No one is in charge to lead efforts to protect information infrastructure against cyber attacks or to lead response and recovery.

Another consequence of this leadership vacuum at DHS is an unclear, uncoordinated strategy for cyber security. The agency has pushed plenty of paper on the topic but people responsible for securing information technology in government, public and the private sector would be hard pressed to identify the top DHS priorities.

The threats to information security are real. Digital systems underpin vital infrastructure throughout the nation and a major disruption to, or widespread lack of confidence in these systems could have a devastating effect on our citizens, our economy and security. The real need is for concrete action guided by a few key national priorities understood by those who must ensure cyber security. DHS needs to immediately fill the position for Assistant Secretary for Cyber Security and Telecommunications to crystallize a few key priorities, and develop programs that support and achieve those priorities.

An important role for the new Assistant Secretary will be ensuring that priorities for cyber security reflect the fact that all critical functions of all industry sectors rely on IT and telecommunications. Coordination and leadership should be the primary concern for DHS.

Lastly, DHS and the White House can take steps to consolidate multiple presidential-level advisory bodies in the area of IT and telecommunications. For example, we have NSTAC and NIAC that clearly have overlapping responsibilities and areas of inquiry. These should be

combined to ensure that presidential advice and recommendations are made holistically, looking across key critical infrastructures, and not in separate silos.

DHS needs to specify steps to prevent and/or minimize a massive cyber attack or telecommunications disaster

DHS documents such as the *National Response Plan* and the *National Infrastructure Protection Plan* attempt to not omit any unconsidered detail. Virtually no agency, program or initiative is left unmentioned in sweeping surveys of the cyber security landscape. The downside to this ocean of detail is that every point seems equally important. Lack of prioritization makes it difficult for organizations to take practical coordinated action to secure their information systems.

CSIA believes this lack of prioritization dilutes the Department's limited resources and makes it less effective in preparing the nation against a massive attack. DHS should articulate a smaller set of priorities focused on preventing and/or minimizing the likelihood or severity of a massive cyber attack or telecommunications disaster.

Creating cyber security for critical systems entails using a combination of technological solutions and best practices for IT. With regard to cyber security technology, its successful use is linked to understanding vulnerabilities of operating systems, applications, networks, and literally thousands of protocols that enable modern IT. Acquiring this knowledge is a moving target due to the complex interdependencies of these technologies and their continuous evolution.

There are 4 major areas of logical activity that DHS should crystallize programs around:

- Risk Management – identification and classification of Critical Infrastructure
- Research & Development – solutions to identify, prevent and recover from attacks
- Incentives – encourage problems to be resolved, not postponed
- Insurance – ensures continuing US financial viability after a cyber loss

<u>Risk Management</u>

An important starting place is for DHS to encourage organizations to pursue cyber security as they would manage other types of risks. In evaluating the nation's IT resources, DHS should help identify the most critical interdependencies and urge organizations to concentrate on protecting those systems first. One positive effort underway is the partnership between DHS and the private sector in developing a protection plan for the IT infrastructure. Under the plan, the private sector is identifying common risk-management processes and techniques. However, this effort is lacking senior-level attention at DHS.

<u>Research & Development</u>

DHS could play a major national role by funding cyber security research and development (R&D) in the private sector. Instead, more than 98 percent of last year's $1.039 billion science and technology budget of DHS went to R&D on weapons of mass destruction. Less than 2% ($18 million) was for cyber security, and of that only about $1.5 million was for basic research.[1]

[1] See CSIA Policy Briefing, "Federal Funding for Cyber Security R&D" (July 2005).

We understand the concern about threats to physical security, but CSIA believes DHS has inadvertently placed the nation in the way of another harmful vector by virtually ignoring R&D on cyber security.

Where DHS has spent money on cyber security R&D there has been some success. Over the past 18 months, the Department's Science and Technology (S&T) Directorate has participated in a technology demonstration project with the Oil and Gas sector. The project, entitled LOGIIC – Linking the Oil and Gas Industry to Improve Cybersecurity – is a public-private partnership between DHS, several companies from the oil and gas sector, process control system (PCS) and information security technology vendors, and the National Labs. This project is aimed at reducing vulnerabilities in process control environments used in the oil and gas sector by establishing a framework for assessing risks, evaluating new technologies, integrating these new technologies into a test environment, and demonstrating commercial event detection and correlation technologies that can significantly enhance situational awareness on PCS networks used in refineries and other large industrial facilities.

There is strong historical precedent for federally funding R&D for emerging technologies of national significance. The Internet is the most famous example, beginning with seed money in 1962 from with the Defense Advanced Research Projects Agency's (DARPA). The Internet is now a vital global infrastructure almost entirely owned and operated by the private sector. Other examples of federal funding for R&D that resulted in important innovations for cyber security include firewalls, intrusion detection systems, fault tolerant networks, open operating systems, cryptography and advanced authentication. CSIA urges DHS to shift a larger portion of its R&D budget to programs that will bolster national cyber security.

Incentives

The time-tested government practice of offering incentives for private investment is another avenue worthy of examination by DHS. By offering incentives such as tax credits for implementation of security solutions, the federal government could dramatically accelerate adoption of measures to shore up national cyber security – just as it has done to spur other initiatives deemed as important for the country by Congress. The key is to develop very carefully-crafted incentives targeted at high priority systems such as certain SCADA systems and Internet security protocols. Many SCADA systems operate on unsupported application platforms and must be moved to a virtual "sandbox" to remediate immediate and urgent security threats.

Insurance

On a related non-technical note, insurance is a practical way for organizations to recover from catastrophic loss. Private insurance policies, however, do not usually provide "cyber risk coverage" due to the newness of this concept and lack of data enabling insurers to establish actuarial loss tables and a viable premium structure. To be effective, premiums for cyber attack coverage would have to include natural risk management incentives for organizations to balance the cost of premiums against the cost of taking preventative measures for security. CSIA believes DHS, in partnership with the Department of Commerce, should sponsor research into viable uses of private-sector insurance coverage for cyber attacks.

DHS has not specified how it will work with the private sector to a cyber incident of national significance

The other major yet unarticulated priority for DHS is describing how it will work with the private sector to respond to and recover from a massive failure of information technology systems – whether from a cyber attack or a natural disaster. This issue is important because it's the private sector – not DHS – that owns and operates information technology systems for most of the nation's critical infrastructure. The unanswered question affecting all is: What is a suitable role for DHS as well as other key federal agencies, including DoD and the FCC in facilitating recovery and reconstitution from a cyber incident of national importance?

DHS is well aware that the private sector "runs the show," which may account for its encouragement of public-private partnerships. I am sure that everyone involved with the multitude of DHS-sponsored public-private partnerships participates with the best of intentions, but there is a lack of clarity in what this work is accomplishing. The Government Accounting Office recently reported that progress on those initiatives is limited, some lack time frames for completion, and relationships between these initiatives are unclear.[2]

Consequently, DHS needs to articulate a chain-of-command for each step of recovery and reconstitution. For example, the DHS's U.S. Computer Emergency Readiness Team (US-CERT) may be aware of a network attack, but the North American Network Operators Group (NANOG) is the operational forum for backbone/enterprise networking. Considerations for this type of situation include:

- Which entity should be in charge of coordinating the actual work of recovery and reconstitution?
- What, if any, related legal authority is possessed by DHS and the federal government?
- What obligations do private sector entities have to obey directives from DHS?
- Who would resolve conflicting demands for scarce cyber resources?
- What enforcement power does DHS have in the process of helping the nation recover from a cyber disaster?

In this context, I would note that DHS in February sponsored "Cyber Storm," a large-scale exercise focused on some of these questions. CSIA and its members supported the exercise but some six months after the event, DHS's after action report containing lessons learned has not been shared with key owners and operators in the private sector.

In addition to chain-of-command, DHS needs to articulate an emergency communications system that works even when standard telecommunications and Internet connectivity are disrupted. Emergency communications entail more than simply establishing a resilient mechanism allowing people to talk. It also requires advance identification of the right people from appropriate organizations who speak the "same language" for establishing rapid recovery and reconstitution of national systems.

[2] "Challenges in Developing a Public/Private Recovery Plan," GAO-06-863T (July 28, 2006).

These are but a few of the details that must be articulated and agreed upon in advance if the nation is to truly prepare for recovery and reconstitution from a cyber disaster. Ostensibly, DHS would have a leading role in planning.

These issues should be answered in the DHS's 400-plus page *National Response Plan*. Unfortunately, the plan does not articulate clear answers on how federal agencies work with each other, with other government entities, or with the private sector in responding to a national disaster. Instead of one coordinator, there are at least six: Homeland Security Operations Center, National Response Coordination Center, Regional Response Coordination Center, Interagency Incident Management Group, Joint Field Office, and Principal Federal Official. The *National Response Plan*'s discussion of cyber security is contained in the "Cyber Incident Annex." The Annex mentions many other federal departments and agencies with "coordinating" responsibility for cyber incident response, including Defense, Homeland Security, Justice, State, the Intelligence Community, Office of Science and Technology Policy, Office of Management and Budget, and State, Local, and Tribal Governments. The agency tasked with maintaining the *National Response Plan* is FEMA.

As I draw toward the end of my testimony, I wish to comment on one other topic that also requires close coordination of the government and private sector – namely, the need for a cyber early warning system that provides the nation with situational awareness of attacks. DHS has sponsored some mechanisms toward this end, such as US-CERT, and Information Sharing and Analysis Centers (ISACs) that share some cyber alert data from the private sector with the federal government. As noted by the Business Roundtable, however, the nation lacks formal "trip wires" that provide rapid, clear indication that an attack is under way.[3] This mechanism would be akin to NOAA's National Hurricane Center, which usually can provide a day or so of advance notice before a dangerous storm lands ashore. Cyber attacks often provide far less notice to prepare and react. DHS should lead the establishment of an efficient national cyber warning system because the private sector is most likely to first detect an attack, and data correlation and follow through coordination closely involves the government.

Summary of Recommendations

In summary, CSIA offers the following recommendations for the Subcommittee's consideration:

Increase Attention to Cyber Security. DHS has inadvertently exposed the nation to another vector of attack by providing inadequate attention to cyber security. The Department should carefully assess its priorities to achieve more balance by shifting some attention from an almost exclusive focus on physical security.

Appoint a Leader. There is no leader at DHS who is solely responsible for cyber security. DHS should swiftly fill the open position of Assistant Secretary for Cyber Security and Telecommunications to close the leadership vacuum.

[3] Business Roundtable, "Essential Steps to Strengthen America's Cyber Terrorism Preparedness" (June 2006); see also Section 15 of Homeland Security Presidential Directive 5, "Management of Domestic Incidents" (Feb. 28, 2003), and the *National Strategy to Secure Cyberspace* (Feb. 2003).

Plan to Prevent or Minimize a Major Cyber Disaster. DHS is too preoccupied with appearing to be in control of every detail related to cyber security. DHS should shift this energy to articulating a smaller set of priorities focused on preventing and/or minimizing the likelihood or severity of a massive cyber attack or telecommunications disaster.

Plan to Work with the Private Sector to Recover from a Major Disaster. The existing DHS "plan" for recovery cites more than a dozen federal departments and agencies with "coordinating" responsibility – not including state, local and tribal governments. DHS needs to clearly articulate a chain-of-command between government and the private sector for recovery from a major cyber disaster.

With that, I appreciate the opportunity to testify today and am pleased to answer your questions.